

Deterministic Client-Side Computational Standard

Zero-Trust Data Sanitization (ZTDS) in Enterprise GenAI

How Fortune 500 CISOs deploy Large Language Models, Multi-Agent Loops, and RAG Pipelines with **Mathematically Provable Zero Data Egress** and **Zero SaaS Subprocessor Liability**.

DATA EGRESS

0.00 Bytes

Client volatile RAM only

SANITIZATION LATENCY

< 1.8 ms

100x faster than cloud DLP

GDPR COMPLIANCE

Art. 28 Exempt

Zero subprocessor chain

OFFLINE ATTESTATION

Ed25519 Token

Zero telemetry heartbeats

The 4 Regulatory & Architectural Chokepoints

Connecting enterprise workflows to cloud AI or local RAG without deterministic pre-egress sanitization triggers severe statutory liabilities:

CHOKEPOINT 01

EU Regulation 2016/679

GDPR Article 28: Subprocessor Trap

Routing cleartext prompts through cloud AI vendors or proxies legally classifies them as data processors. Requires 30-day customer notification windows, complex DPA redlines, and unlimited cross-border transfer risk.

CHOKEPOINT 02

GDPR Art. 17 / Data Erasure

Vector Database Poisoning

Cleartext PII converted into high-dimensional vector embeddings cannot be deleted upon user "Right to Erasure" request without destroying and re-indexing the entire multi-million vector index.

CHOKEPOINT 03

EU AI Act (2024/1689)

Article 50: Synthetic Provenance

Mandates verifiable provenance and transparency for high-risk generative AI pipelines. Penalties for unverified sensitive data ingestion reach up to €35,000,000 or 7% of global annual turnover.

CHOKEPOINT 04

US HIPAA & FRE Rule 502

Loss of Clinical & Legal Privilege

Transmitting unmasked PHI violates HIPAA Safe Harbor (45 CFR § 164.514) triggering mandatory BAA audits. Sending unredacted M&A contracts or litigation notes waives Attorney-Client Work Product Privilege.

Why Legacy Cloud DLP Proxies Break Generative AI

Cloud DLP solutions (Netskope, Nightfall, AWS Macie) were engineered for asynchronous email archiving, not sub-second multi-agent LLM reasoning chains:

Architectural Vector	Legacy Cloud DLP Proxy (SaaS)	ZTDS RFC v1.0 Local Engine
Execution Latency	250 ms – 800 ms (Network roundtrip)	< 1.8 ms (Local CPU/RAM)
Data Egress Boundary	Transmits cleartext to 3rd-party cloud	0.00 Bytes (Stays in local host memory)
Subprocessor Chain	Adds another SaaS vendor (+ DPA & SOC2)	Exempt (Self-contained computational utility)
LLM Context Preservation	Destructive masking ([REDACTED] breaks syntax)	Deterministic surrogate tokens ([EMAIL_1])
Air-Gapped / SCIF Support	Impossible (Requires active internet connection)	100% Offline (Ed25519 cryptographic token)

- The 10-Agent Latency Tax: A multi-agent loop with 12 sequential LLM steps wastes **6,000 ms** with cloud proxies vs. **21 ms** with ZTDS.

The 4 Fundamental Invariants (RFC v1.0)

DOI: 10.5281/zenodo.22058770

1 ZERO EXTERNAL EGRESS

Raw PII, PHI, or intellectual property never crosses the local execution boundary in cleartext. Sanitization occurs strictly prior to socket write.

Formula: $\Delta_{\text{Egress}}(\text{Cleartext}) \equiv 0.00 \text{ Bytes}$

2 DETERMINISTIC TOKENIZATION

Masked entities are replaced with bijective surrogate tokens preserving grammatical syntax, entity classes, and token distance for optimal LLM attention weights.

Map: $T = M(V, C) \mid \text{Scoped strictly to Thread RAM}$

3 CRYPTOGRAPHIC ISOLATION

Execution is verified inside volatile RAM or hardware-attested enclaves (AWS Nitro, Apple Secure Enclave, WASM sandbox) with zero disk swapping.

Memory: Zero Persistence, Instant Auto-Zeroization

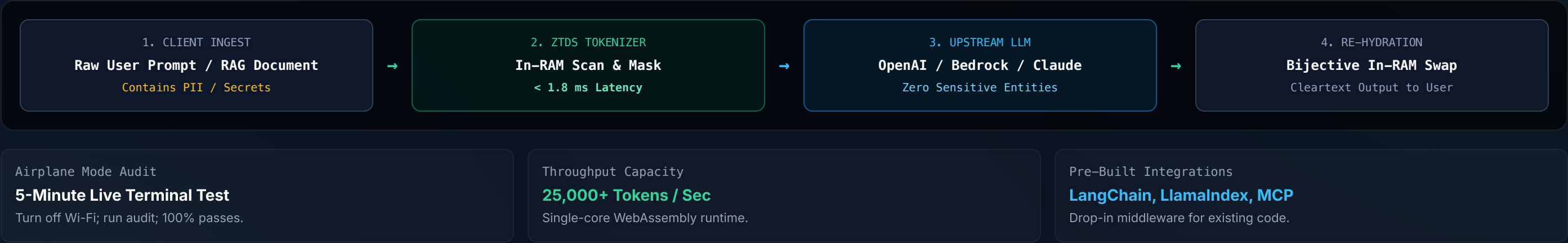
4 CONTINUOUS COMPLIANCE

Software operates as an endpoint utility. Completely eliminates third-party subprocessor status under GDPR Article 28 and HIPAA Business Associate rules.

Legal Status: 100% DPA & BAA Exemption

Sub-Millisecond Bijective In-Memory Architecture

Zero cleartext entities reach the upstream network. All de-identification and re-hydration occur within host process RAM:



Why Enterprise Legal Clears ZTDS in 48 Hours

Traditional software procurement stalls over Data Processing Agreements (DPAs) and liability caps. ZTDS is legally exempt by architectural design:

EDPB DOCTRINE & GDPR

Article 28 Exemption

Under European Data Protection Board doctrine, local computational utilities executing in client volatile memory do not constitute "data processors". No DPA or Standard Contractual Clauses (SCCs) are legally required.

US HHS / HIPAA

Safe Harbor De-identification

Under 45 CFR § 164.514, clinical text stripped of the 18 designated identifiers ceases to be PHI. Because masking occurs prior to network dispatch, neither ZTDS nor the LLM handles PHI. No BAA required.

AICPA SOC 2 TYPE II

Automated Evidence Binder

Direct export of ztds-evidence-binder.json mapped to Common Criteria CC6.1 (Access), CC6.6 (Perimeter), and CC6.8 (Malicious Code) ready for Drata, Vanta, and AuditBoard ingestion.

Turnkey Deliverable: Official 1-Page CISO Exemption Memorandum ready for your General Counsel and DPO sign-off.

Zero DPA Overhead

Offline Ed25519 Licensing & True Air-Gapped Enclaves

Regulated SCIF environments, defense systems, and sovereign cloud VPCs strictly prohibit software that "phones home". ZTDS enforces offline cryptographic licensing:

Cryptographic Token Spec (Ed25519)

```
ZTDS-LIC-v1.eyJjdXN0b21lcklkIjoiQUNNRS1DT1JQIiwidGllciI6IkV0VEVSUFJJU0VfQUlSIiwibm9kZXMiOjUsInByb2ZpbGVzIjpbIioiXX0.k9F...b9a
```

- In-Memory Verification: **111.8 microseconds** (~0.1ms)
- Network Egress / Heartbeats: **Exactly 0.00 Bytes**
- Native Node.js & WebAssembly crypto engine

Enterprise Operational Guarantees

- ✓ **Zero Pipeline Disruption:** Built-in 60-day automatic grace period ensures mission-critical workflows never halt if annual renewal PO is in processing.
- ✓ **Tamper-Proof Integrity:** Any modification to customer ID, node count, or profiles mathematically invalidates the signature.
- ✓ **Hardware Enclave Compatible:** Deploys natively in AWS Nitro Enclaves, Azure Confidential Computing, and Kubernetes VPCs.

```
CLI: npx ztds-audit --check-license
```

The 25 High-ACV Specialized Industry Profiles

Generic regex produces unacceptable false positives. ZTDS combines context heuristics with algorithmic checksum validation (Luhn, ISO 7064 Mod 97-10, Verhoeff):

HEALTHCARE / PHI

- 18 HIPAA Identifiers
- ICD-10 / ICD-11 Codes
- Physician NPI Numbers
- Clinical Trial Hashes
- Genomic Identifiers

FINANCIAL & BANKING

- PCI DSS PAN (Luhn)
- SWIFT / BIC Codes
- IBAN Numbers (ISO 7064)
- CUSIP / Bloomberg ID
- SEC 13F Holding Data

LEGAL & M&A SECRECY

- Acquisition Target Entities
- Attorney Work Product (FRE 502)
- Executive Comp Plans
- Board Resolution Drafts
- Subpoena Docket Hashes

CLOUD & INFRA SECRETS

- AWS IAM & Secret Keys
- GitHub Personal Tokens
- Kubernetes JWT Tokens
- Private RSA/Ed25519 Keys
- Database Connection URIs

Anti-Cannibalization Model: Free standard handles basic consumer PII. The 25 high-ACV profiles require signed Enterprise tokens.

Quarterly Regulatory Taxonomy Updates

Commercial Subscription Tiers & TCO Economics

Transparent annual flat-rate licensing without opaque consumption-based per-token penalties:

DEVELOPER PRO SDK \$1,990 / Year - Up to 5 Developer Seats & Nodes - Baseline universal consumer PII - LangChain, LlamaIndex, MCP connectors - Standard engineering support (48h SLA) AI Engineering Teams	
ENTERPRISE AIR-GAPPED \$12,000 / Year - Up to 5 Production Nodes / Enclaves - Full 25 Specialized Industry Profiles 100% Disconnected Ed25519 Token - SOC 2 Type II Evidence Binder - Priority support (4h response SLA) Core Enterprise VPCs	RECOMMENDED

GLOBAL SITE LICENSE \$50,000 / Year - Unlimited global nodes & enclaves - Custom ERP/CRM profile engineering - Direct advisory with Chief Architect - Air-gapped source code escrow rights 24/7 critical incident response (1h SLA)	
---	--

EVALUATION PROTOCOL

Frictionless 14-Day Sandbox Pilot to Production

TCO Comparison: In-house custom build: \$350k+ in salaries. Cloud DLP SaaS: \$120k+/yr + 400ms latency. ZTDS: \$12k/yr turnkey.

Standard Form: docs/legal/ENTERPRISE_ORDER_FORM_TEMPLATE.md

Fixed Annual Price

The 14-Day Turnkey Evaluation Roadmap

Zero technical friction and zero upfront commitment. Prove compliance inside your private network before signing:

DAY 1

5-Min Verification

Run `npx ztds-audit` on your workstation. Inspect network traffic with Wireshark/DevTools. Confirm 0 bytes egress.

DAYS 2 – 10

Air-Gapped Sandbox

Deploy 14-day evaluation license token into your staging VPC or Nitro Enclave. Benchmark 25 profiles against real payloads.

DAYS 11 – 12

Fast-Track Clearance

Deliver 1-Page DPA Exemption Memo to Legal. Ingest SOC 2 Type II Evidence Binder into Drata / Vanta.

DAY 14

Production Token

Execute Schedule A Order Form (Net 30 terms). Production Ed25519 token delivered via PGP within 2 business hours.

Initiate 14-Day Enterprise Sandbox Pilot Today

Direct contact with Chief Architect Ilya Sibiryakov · BrandMeWeb Ecosystem

Request Sandbox Token →